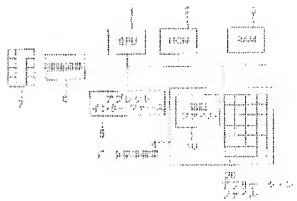
AUTHENTICATION IC CARD

Publication number: JP2000132658 (A)
Publication date: 2000-05-12
Inventor(s): HOKURA YUTAKA +
Applicant(s): HOKURA YUTAKA +
Classification:
- international: ***G06K19/10;*** **G06K19/10;** (IPC1-7): G06K19/10
- European:
Application number: JP19980299181 19981021
Priority number(s): JP19980299181 19981021

Abstract of **JP 2000132658 (A)**

PROBLEM TO BE SOLVED: To obtain an IC card where the authentication of qualified person is integrated concerning plural transaction objects for the security of transactions and by which the privacy for information stored in the IC card itself is surely protected. SOLUTION: The IC card is provided with 2 CPU 1, an authentication file 10 storing individual identification information and an application file 20 classified in accordance with the depth of the authentications. When the presentation of information recorded in the application file 20 is requested from an external part, individual identification information inputted from the external part is compared with that stored in the authentication file 10, the depth of the authentication is recognized and information of the application file 20 is presented through the CPU 1 for the first time at the time of passing in the authentication IC card. Individual identification information can be biological information for discriminating the individual of an owner.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－132658
（Ｐ2000－132658Ａ）
(43)公開日　平成12年５月12日(2000.5.12)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｓ　５Ｂ０３５

審査請求　有　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平10－299181

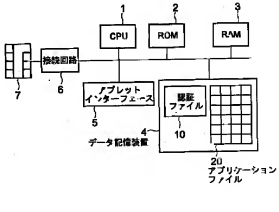
(22)出願日　平成10年10月21日(1998.10.21)

(71)出願人　393031796
保倉　豊
千葉県八千代市勝田台南２丁目15番22号
(72)発明者　保倉　豊
千葉県八千代市勝田台南２丁目15番22号
(74)代理人　100104341
弁理士　関　正治

Ｆターム(参考)　５Ｂ０３５　ＡＡ０２　ＡＡ０６　ＡＡ１４　ＢＢ０９　ＢＣ００
ＢＣ０１　ＢＣ０２　ＢＣ０３　ＢＣ０６　ＣＡ１１
ＣＡ２２　ＣＡ２３　ＣＡ２５　ＣＡ２９　ＣＡ３８

(54)【発明の名称】　認証ＩＣカード

(57)【要約】
【課題】　取引のセキュリティのために複数の取引対象についての資格者認証を統合した認証ＩＣカードを提供し、またＩＣカード自体に格納する情報に対するプライバシー保護が万全な認証ＩＣカードを提供する。
【解決手段】　ＣＰＵと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えて、外部からアプリケーションファイルに記録された情報の提示要求があったときに、外部から入力される人証情報と認証ファイルに格納された人証情報と対比して認証の深さを確認し、合格したときに初めてＣＰＵを介してアプリケーションファイルの情報を提示するようにした認証ＩＣカード。なお、人証情報は所有者の個体を区別する生物学的情報であってもよい。



【特許請求の範囲】

【請求項1】　CPUと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えた認証ICカードであって、外部から前記アプリケーションファイルに記録された情報の提示要求があったときに、前記CPUが外部から入力される人証情報と前記認証ファイルに格納された人証情報と対比して認証の深さを確認し、合格したときに前記CPUを介して前記アプリケーションファイルへのアクセスが認められることを特徴とする認証ICカード。

【請求項2】　CPUと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えた認証ICカードであって、外部から前記アプリケーションファイルに記録された情報の提示要求があったときに、前記CPUが前記認証ファイルに格納された人証情報を出力して、外部装置から受け取る判定結果に基づいて、前記CPUを介して前記アプリケーションファイルへのアクセスを行うことを特徴とする認証ICカード。

【請求項3】　前記人証情報が該ICカードの真正な所有者の個体を区別する生物学的情報を含むことを特徴とする請求項1または2記載の認証ICカード。

【請求項4】　前記アプリケーションファイルには対象とする取引の権限を示す固有のIDが記録してあることを特徴とする請求項1から3のいずれかに記載の認証ICカード。

【請求項5】　前記アプリケーションファイルには所有者の個人的情報が記録してあることを特徴とする請求項1から4のいずれかに記載の認証ICカード。

【請求項6】　前記アプリケーションファイルへのアクセスは、ファイル毎に予めアクセス資格を登録し、認定された資格者に対してのみ認めるようにしたことを特徴とする請求項1から5のいずれかに記載の認証ICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子情報交換や電子商取引における個人認証を行うため認証票として用いる認証ICカード、あるいは格納した個人情報を提示するときに適切な保護ができるようにした認証ICカードに関する。

【0002】

【従来の技術】近年、研究所や事業所、研究室、資料保管室さらに住宅など、セキュリティの確保のため特定の場所に出入りできる者を限定し、有資格者に発行したカードによる認証に合格した場合だけ開錠する施錠管理システムがよく用いられている。また、商品の販売やクレジットなどの電子商取引、医療におけるオンライン診察、個人カルテや役所における登録事項の閲覧、証明書の発行など、本人にのみ取引を認めるべき場合に本人認証を正確に行う必要がある。さらにこのような場合に対面して取引を行うのでなく、通信網を利用して情報にアクセスする機会が多くなりかつ多様化している。

【0003】こうした取引では真正な取引対象者であるか否かを判定しなければならず、また、場合によっては対面交渉なしに本人であるか否かを正確に判断できなくてはならない。これらの場合、カードを仲介にして本人認証を行うことで信頼性を向上させることができる。なお、取引の種類により要求されるセキュリティの程度が異なるため、本人認証の深さが異なる。たとえば少額商品を購入する場合にはカードの純正が保証できれば満足できても、運転免許証の発行に利用する場合は確実に本人であることが証明できる顔写真、指紋、声紋などの生物学的情報を併用することが好ましい。

【0004】入退場管理に用いられるカードは、通常従前毎に発行され、有資格者が所持あるいは管理する。したがって多数の部屋などを入退場管理の対象とする場合は、高度の資格者は多数の鍵カードを所持しなくてはならず管理が煩雑になる。なお、1枚のカードを有資格者が共有して利用することも多いが、この場合は暗証番号やカードの管理を厳重に行わなければ認可されていない者の盗用を許すことになり、かえって安全の保持が困難になる。また、取引用カードも取引者間で合意の下に発行されるものの、個人が所有するカードの数はいつの間にか膨大な数になってしまうきらいがある。

【0005】一方、近年ICカードなどにCPUと記憶装置を内蔵するカードをクレジットカードや電子マネーなどに利用するようになってきた。ICカードは高度な認証に伴う複雑な演算も可能であり記録内容の書き換えが容易であることが特徴で、取引の経緯を逐次記録できるカードや電子マネーとして使用することなどに適している。また、ICカードなどに内蔵される記憶容量が大きくなってきたため、カード自体に各種の個人的情報を記録して携帯することも可能となっている。常時携帯することが便利な個人的情報には保険証番号、クレジットの利用者番号、社員証番号や社内における経歴、電子マネー残額、戸籍簿の内容、病歴、さらに住所録など、プライバシーに係わり他人に漏洩しないという保証がない場合には利用を認めるべきでないものがある。

【0006】

【発明が解決しようとする課題】そこで、本発明が解決しようとする課題は、取引や施錠システムのセキュリティ向上のために対象毎に発行してきた認証カードを資格者認証として統合した認証ICカードを提供することである。本発明が解決しようとする別の課題は、ICカード自体に格納する情報に対するアクセスの安全が保証されたプライバシー保護が万全な認証ICカードを提供することである。

【0007】

【課題を解決するための手段】上記課題を解決するた

め、本発明の認証ＩＣカードは、ＣＰＵと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えた認証ＩＣカードであって、外部からアプリケーションファイルに記録された情報の提示要求があったときに、外部から入力される人証情報と認証ファイルに格納された人証情報と対比して認証の深さを確認し、合格したときに初めてＣＰＵを介してアプリケーションファイルの情報を提示することを特徴とする。

【０００８】従来、認証が必要となる場面毎に独立したカードを発行して対処してきたのは、その方がシステムとして単純で扱いやすいこと、多様な取引者同士の提携が困難なことなどの理由の他に、取引により必要とされる認証の深さが異なり一様な人証情報では対処できないこと、１枚のカードで複数の取引を可能とするとカード所有者に認めたくない資格権限を与えることになる場合が生ずることなどの技術的な障害もあったからである。

【０００９】本発明の認証ＩＣカードによれば、カード内のアプリケーションファイルをファイル毎に機密性に対応した認証の深さに応じて分類しておき、外部からファイルに記録された情報の提示要求があったときには、入力される人証情報をＣＰＵが対照確認し、ファイルについて予め決められた深さに対応する認証が得られたときにのみＣＰＵを介して目的のアプリケーションファイルの情報を提示するようになっている。

【００１０】また、カードの携帯者により入力された人証情報とカード内部に記録された人証情報の照合は、外部装置によって行うこともできる。外部装置の能力を利用することにより、複雑な画像処理や情報処理を必要とするときにも対処できるので、認証ＩＣカードのＣＰＵ能力やメモリ容量では不足がある場合などに有効である。なお、認証ファイルに格納される人証情報はＩＣカードの真正な所有者の個体を区別する生物学的情報を含むようにすることができる。

【００１１】また、認証の深さで分類されたアプリケーションファイルには各種取引に用いられるＩＤを記録しておってもよい。このようなＩＤは、外部に取引情報が存在する場合などにおいて、カードの携帯者がこれにアクセスする資格を有するか否かを検証する必要がある場合に有効である。さらに、アプリケーションファイルに所有者の個人的情報を記録しておいてもよい。本発明の認証ＩＣカードの認証能力は高く本人の承認なしではカード内の個人的情報にアクセスできないので、プライバシーの保護は万全である。また、アプリケーションファイル毎に予めアクセス資格を登録し、認定された資格者しかファイルへのアクセスを認めない機構を併用しても良い。認証レベルと組み合わせてファイルを２次元的に配設することができるので、より複雑な要求に応えることが可能となる。

【００１２】本発明の認証ＩＣカードを使用するときは、まず認証ＩＣカード中のアプリケーションファイルに入室許可証、銀行のＩＤなどを格納すると共に、それぞれが要求する認証方法を指定しておく。一方、認証に必要な人証情報を認証ファイルに格納しておく。たとえば、建物の入場には特別な認証は必要なく適正な認証ＩＣカードを所持していればよいとし、執務室への入室には認証ＩＣカードと共に保持者の真正を確認するための暗証番号が合致しなければならないとし、さらに、資料室への入室には より厳密な認証が要求され各人の指紋を照合するものとする。

【００１３】このような場合、認証ファイルに、純正なカードであることを示す情報と、暗証番号と保持者の指紋情報を記録しておき、アプリケーションファイルの各々に、建物の入口扉を開扉するために要求される暗号信号と執務室の開扉に必要な暗号信号と資料室の扉を開扉する暗号信号を格納しておく。

【００１４】カードの携帯者が建物の扉に付属するカード読み取り器に認証ＩＣカードを読み取らせると、カード読み取り器がカード情報を取得してカードが真正であって暗号が一致することを確認し、検査に合格したときに扉が開き入場できる。執務室の扉に設けられたカード読み取り器にはキーボードが付属していて、入室しようとする者は認証ＩＣカードを読み取らせて暗証番号を入力する必要がある。認証カードが真正で暗証番号が認証ＩＣカードの認証ファイルに記録された暗証番号と合致したときに、ＣＰＵを介して開扉に必要な暗号信号がカード読み取り器に送り込まれ、これが正しければ入室が許可される。

【００１５】また、資料室の扉には指紋読み取り装置を付属したカード読み取り器が設けられていて、入室しようとする者は真正な認証ＩＣカードをカード読み取り器に読み取らせて指定された指を指紋読み取り装置に押し付ける必要がある。指紋が認証ファイルに記録された指紋情報と対応する場合に、ＣＰＵを介して開扉を指示する暗号がカード読み取り器に供給され、この暗号信号がカード読み取り器により真正な者と判定されたときに始めて扉が開いて入室ができる。

【００１６】同じ仕組みが、金融システムにおいても使用される。クレジットを使用する場合にも、低額商品の購入にいちいちサイン入力を要求するのでは煩雑に過ぎて利用価値が減少する。一方、宝飾類など高額な取引では厳重な本人認証を行う必要がある。クレジットの利用者認証番号をアプリケーションファイルから出力するにも要求される認証水準が異なるが、本発明の認証ＩＣカードでこれら異なる水準の認証に対応することができる。

【００１７】また、アプリケーションファイル毎に予めアクセス資格を登録し、認定された資格者しかファイルへのアクセスを認めないようにして、カード読み取り器からの情報アクセスを必要な部分に制限して余分なプラ

イバシー開示を行わないようにすることができる。たとえば解錠システムが要求できる情報は人証情報と解錠のための暗号信号だけで、医療カルテが格納されているファイルに対するアクセスはＣＰＵによって排除される。場合によっては、不当なアクセス要求があったときには情報交換全てを遮断して情報窃取や改竄を防止するようにすることができる。

【００１８】本発明の認証ＩＣカードは、サービスや取引（以下代表して取引と呼ぶ）毎に利用資格を与えられた者が所持する認証ＩＣカードにその取引を認めるための暗号信号を記録しておき、取引を行うときに認証ＩＣカードの携帯者が真正な所持者であることを確認して取引を認める仕組みである。したがって、サービス等の提供者が認証ＩＣカードから受け取るべき情報は、認証ＩＣカードの携帯者がカードの真正な所有者であることと認証ＩＣカードに利用資格を有する証拠となる暗号信号が記録されていることである。また、認証ＩＣカードが認証することは、読み取り装置が適正なものであることと携帯者が真正な所持者であることである。

【００１９】本発明の認証ＩＣカードでは、建物への入場や為る資料室への入室の資格、銀行の口座、クレジットの所有、さらに戸籍、履歴や、電子マネーとして利用する場合の与信残高などを含め、いわば所持者の属性を認証ＩＣカードに収納することにより、利用資格が与えられた全ての取引の認証を１枚のカードに統合することができる。

【００２０】すなわち、本発明の認証ＩＣカードは、取引資格をカードに与えるのではなくカードの所有者個人に与えるものであるから、従来のカードシステムより本来の信認目的に沿った運用を行うことができる。したがって、従来のようにサービス毎に支給されたカードを多数携帯している必要がなく、従来の多人数で共有する解錠用カードのようにカード自体を他人が利用しないように厳重に管理する必要もない。

【００２１】

【発明の実施の形態】以下、図面を参照して本発明の詳細を実施例に基づいて説明する。図１は本発明の実施例の認証ＩＣカードの構成を示すブロック図、図２は本実施例におけるファイル構成を示すブロック図、図３は本実施例の使用例を示すブロック図、図４は本実施例の使用例を示す流れ図である。

【００２２】

【実施例】本実施例の認証ＩＣカードは、図１にあるように、情報処理を実行するＣＰＵ１、情報処理プログラムを収納したＲＯＭ２、演算用データを記憶するＲＡＭ３、情報の書き込み読み出しが可能なデータ記憶装置４、アプレットプログラムに対するインターフェース５、外部接続用接続回路６、および外部接続端子７を備える。データ記憶装置４のファイルには、認証データを記憶した認証ファイル１０と、外部とやり取りする情報を格納したアプリケーションファイル２０が含まれる。

【００２３】なお、外部接続端子７は、信号伝達および電源の供給に用いられるが、非接触型の電極やアンテナであっても良い。また、各種のカード読み込み装置に対応するため接触型と非接触型の両方の接続端子を備えるようにしても良い。アプレットインターフェース５は、外部から小型プログラム（アプレット）を受け入れてそのプログラムに従ってＣＰＵを作動させる場合に用いるもので、受け取ったアプレットが認証ＩＣカードにとって無害であることを認識する機能を備えたインターフェースである。安全のため認証ＩＣカードがアプレットを受け付けないようにしても よく、このような認証ＩＣカードではアプレットインターフェース５も無用である。

【００２４】認証ファイル１０には、認証ＩＣカードが真正であることを保証するためのデータに加えて、認証ＩＣカードの真正な所有者を認証するための人証情報が格納されている。認証は簡単なものから高度な保証を与えることができるものまで段階Ｉ，ＩＩ，ＩＩＩ，・・・を追って複数のものが記録されている。人証情報は、たとえば暗証番号、指紋、声紋、醒写真、サイン筆跡など、本人しか知らないものや生物学的情報で本人以外では再現できないようなものが好ましい。

【００２５】アプリケーションファイル２０は、格納する情報の種類に関する第１の分類と認証に関する第２の分類にしたがって区分されている。すなわち第１分類ａ，ｂ，ｃ，・・・は、例えば住宅管理用情報、医療情報、金融情報、通信情報など、通常は認証を使用するサービス機関を区別するために使用される分類である。第２分類Ｉ，ＩＩ，ＩＩＩ，・・・は、要求される認証の程度に従った分類で、簡単な認証でアクセスを認めるものから、指紋で確認するなど高度な認証に合格して始めてアクセスを認めるものまで認証深さにより分類されたものである。

【００２６】たとえば、ビル管理会社から提供される情報を格納するのは第１分類ｂで、住宅棟の入場許可暗号はその第２分類Ｉのファイルに、クローゼットの開扉暗号は第２分類ＩＩのファイルに、また自室の扉の開扉暗号は第２分類ＩＩＩのファイルに記録されている。なお、これらのファイルには暗号の鍵や電子証明書などを入れておくこともできる。

【００２７】住宅棟の入口にはカード読み取り器が設備されていて、入居者が認証ＩＣカードを読み取り器に読み込ませると、カードと読み取り器の間で相互に真正性をチェックして合格すると扉が開き住宅棟に入ることができる。住宅棟内の各室には既重な扉が付いているため、単に認証ＩＣカードが真正であることを確認するだけの簡単な認証で住宅棟への立ち入りを許可している。なお、認証ＩＣカードがカード読み取り器が真正なものであることを確認する機能を持つのは、認証ＩＣカードに格納されている情報を窃取したり内容の書き換えをす

ることを防ぐ必要があるからである。

【0028】図3は、認証ICカードの利用方法の代表的な例として住宅の入室管理に使用した例を挙げて説明したブロック図である。各室の扉30には扉開閉制御装置31が設備されていて、扉30は通常手で開けることができないようになっている。扉開閉制御装置31には認証制御装置32が接続されていてここから発生される制御信号に従って扉の開閉が行われる。認証制御装置32には入証情報入力装置33とカード読み込み器34が接続されている。

【0029】以下、図4の流れ図を参照しながら、認証ICカードを使用するときの情報処理手順を説明する。入室しようとするカード使用者が認証ICカード35をカード読み取り器34に挿入すると（S1）、認証制御装置32は読み取り器IDを認証ICカード35に送ると共に認証ICカードのIDを問い合わせる（S2）。認証ICカード35は読み取り器IDを認証ファイルの情報と対照して極金し、自己のカードを扱って良いものであることが確認できたときに（S3）、認証ファイルに記録されているカードのIDをカード読み取り器34に返送する（S4）。これらのやり取りは全てCPUを介して行われ、カード読み取り器34は直接的に認証ICカードの記憶装置にアクセスできない。

【0030】認証制御装置32は認証ICカードのIDがシステムに適合した真正なものか否かを判断し（S5）、適合しない場合はカードを排出して拒絶する（S20）。適合している場合には、認証レベルに基づいて決められた例えば指紋など、人証の入力を督促し、使用者が人証情報入力装置33から入力する情報を読み取り（S6）、入力した情報を抽出処理して人証情報を作成する（S7）。

【0031】人証情報が真正か否かを認証ICカード側で確認するか扉開閉制御装置側で確認するかを判定し（S8）、認証ICカード35で確認することになっている場合は、人証情報を認証ICカード35に伝達すると共に扉を開くための開扉暗号を求める（S9）。認証ICカード35は受け取った人証情報を認証ファイルに格納されている人証情報と照合して（S10）、両者が合致すると認められる場合は、所定のアプリケーションファイル（この場合はb11のファイル）に記録されている開扉暗号をカード読み取り器34を介して認証制御装置32に送付する（S11）。

【0032】なお、人証情報が真正か否かを扉開閉制御装置側で確認する場合は、認証ICカード35に対し記録されている人証情報を要求し（S12）、認証ICカード35が回答してきた（S13）人証情報と先に取得したカード使用者の人証情報との照合を行い（S14）、合格したら今度は認証ICカード35に対し開扉暗号を求める（S15）。認証ICカード35は求めに応じて所定のアプリケーションファイルに記録されている開扉暗号を認証制御装置32に送付する（S11）。

【0033】こうして受け取った開扉暗号が真正であれば（S16）、扉開閉制御装置31に開扉指示信号を与えて（S17）扉30の解錠をするので（S18）、認証ICカードの所持者が入室することができる（S19）。

【0034】また、認証ICカード35のデータ記憶装置4の使用領域を少なくするために人証情報を分割して認証ICカード35と認証制御装置32に分納することもできる。この場合は人証入力装置から入力された人証情報と認証ICカード35と認証制御装置32とに分割されて格納されている人証情報とを照合して開扉暗号を出す。このように人証情報を認証ICカード35と認証制御装置32とに分割することは、単にメモリ領域の節約だけでなく、仮に認証ICカードの認証ファイルから人証情報が盗まれたとしてもそれだけからでは照合することができないため、セキュリティ面での効果もある。

【0035】また、上記の例では、認証ファイルに格納される人証情報として3段階使用したが、段階の数はいくつに設定しても良い。人証情報としては、カードの発行者が記入しておくID番号のみに基づいて真正を証明する最も簡単な段階から、カードの所有者が決めた暗証番号、所有者の指紋、虹彩、顔写真などの生体情報、所有者が入力するサインなどの動的情報、さらにこれらを組み合わせたより高度な複合情報などが使用できる。なお、生体情報は真正な所持者の体が生物学的に所有している情報で真似することが困難ではあるが、コピーすることにより成り澄ますことができる。これに対し、現場における本人の動作を伴う動的情報を利用すると成り澄ましが困難になるので、より信頼性の高い認証ができる。

【0036】人証情報入力装置は、サイン入力を要求する場合は図形入力装置、暗証番号を使用するときにはキーボード、指紋を使用するためには指紋取得装置、虹彩を利用する場合は瞳を撮像するカメラと判定装置など、使用する人証情報に応じて、その情報を取得する装置を準備しなければならない。

【0037】また、ICカードに記録された個人的情報をアクセスする場合や、病院でカルテを開示させる場合のように、所持者が認証の深さを指定することが好ましいことがある。例えば住民票を取るときと納税証明を取るときで認証の深さを変えたいと思えば、それぞれの証明を求めるときに使用する暗号番号を格納するアプリケーションファイルの認証深さの指定を変えればよい。医療における支払いをするときと通信網を利用した在宅診療を受けるときでは、本人認証の重要性が異なることは明らかであるが、このような場合にも本発明の認証ICカードは的確に対応することができる。

【0038】なお、1枚の認証ICカードを会員証や社員証、あるいは行政窓口における本人証明カードとして

利用したり、交通機関の定期券、プリペイドカード、クレジットカード、テレホンカード、ショッピングカード、あるいは与信残高金額を書き換えることができる電子マネーとして使用することもできる。また、ホテルなどでチェックイン時に部屋の扉開閉を行う暗号を認証ＩＣカードのファイルに記憶しチェックアウト時に消去するというように、一時的な利用も可能である。

【００３９】

【発明の効果】以上詳細に説明した通り、本発明の認証ＩＣカードは、ＣＰＵを介して情報のアクセスを行うため、ファイルのアクセス権限を任意に設定して、人証情報を活用して正しいアクセスのみを実行するので、所持者のプライバシーが確実に保護でき、またサービスの提供者等にとっても安全性の高い取引が可能となる。また、本発明の認証ＩＣカードは所有者自身の属性を記録したものと見なすことができ、ある個人が有する各種のサービスや取引の利用資格を証明するための認証を統合して実施することができるから、カードの取り扱いが簡単になり、多数のサービス等を利用する場合でも携帯するカードの数を少なくすることができる。

【図面の簡単な説明】

【図１】本発明の実施例の認証ＩＣカードの構成を示すブロック図である。

【図２】本実施例におけるファイル構成を示すブロック図である。

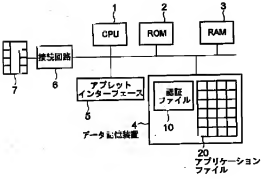
【図３】本実施例の使用例を示すブロック図である。

【図４】本実施例の使用例を示す流れ図である。

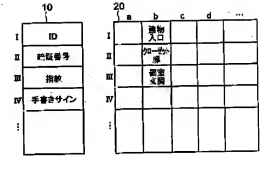
【符号の説明】

１　ＣＰＵ
２　ＲＯＭ
３　ＲＡＭ
４　データ記憶装置
５　アプレットインターフェース
６　外部接続用接続回路
７　外部接続端子
１０　認証ファイル
２０　アプリケーションファイル
３０　各室の扉
３１　扉開閉制御装置
３２　認証制御装置
３３　人証情報入力装置
３４　カード読み込み器
３５　認証ＩＣカード
Ⅰ，II，III，・・・　認証段階に関する第２分類
ａ，ｂ，ｃ，・・・　情報種類に関する第１分類

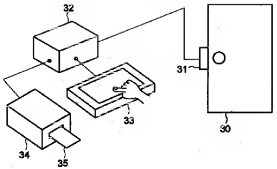
【図１】



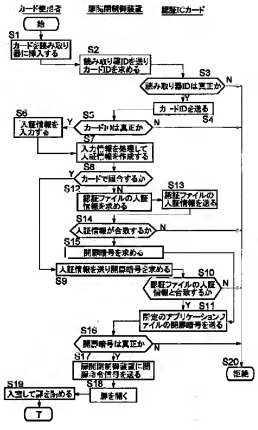
【図２】



【図3】


32
31
33
30
34
35

【図4】


カード使用者
扉制御装置
認証ICカード
始
S1
カードを読み取り器に挿入する
S2
読み取り器IDを送りカードIDを求める
S3
読み取り器IDは真正か
N
Y
カードIDを送る
S4
S5
カードIDは真正か
Y
N
S6
入室情報を入力する
S7
入力情報を処理して入退室条件を決する
S8
カードで届けするか
Y
S12
N
認証ファイルの人脈情報を求める
S13
認証ファイルの人脈情報を送る
S14
人脈情報が合致するか
N
S15
開閉暗号を求める
人脈情報を送り開閉暗号を求める
S9
S10
認証ファイルの人脈情報と合致するか
N
Y
S11
所定のアプリケーションファイルの開閉暗号を送る
S16
開閉暗号は真正か
N
S17
Y
扉制御装置に開扉き命令を送る
S18
扉を開く
S19
入室して閉じるめる
S20
切断
T